An Optimized Steganography Techniques using Hybrid approach

SHORT SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna University

by

Scholar Name: Urmila Pilania
Registration number: 2K16-PFE-23

Under the supervision of

Name of Supervisor: Dr. Prinima Gupta
Designation: Associate Professor
Department of Computer Science & Technology
Faculty of Engineering

MANAV RACHNA
vidyanatarikshah

MANAV RACHNA UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING)
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

Year: August, 2018

MANAV RACHNA
Vidyapatarikshai

MANAV RACHNA UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

DECLARATION BY THE SCHOLAR

I hereby declare that the short synopsis **Title: "An Optimized Steganography Technique using Hybrid approach"** being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in department of **Computer Science & Technology** under Faculty of Engineering of Manav Rachna University, Faridabad during the academic year August, 2018.

It is a bona-fide record of original work carried out under the supervision of **Dr. Prinima Gupta** has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that short synopsis is within the plagiarism limit and copy of the same is attached as per University norms.

URMILA PILANIA Urmila
(Name and signature of the Scholar)
Registration number: 2K16-PFE-23

Prinima 16/8/2018
Signature of the Supervisor
Full name, Designation and Faculty

Susmita Ray
Chairman, DRC

Proposed Title: A Novel Steganography Technique using ROI, IWT and SVD

Abstract: In today's world of internet most of the data travel through internet. It is desirable to secure the information at sender's end till it reaches receiver's end and during transmission. Today everybody is using internet that may be a child or may be an old age person, every professional is using internet to create digital data and that data is shared over the network, as so many people's are using internet so information security has become a prime task. That is why we need some security techniques for safety of information during information travel over the internet. There are some techniques for protection of data like Cryptography, Watermarking, Digital Signature and Steganography. Steganography has been proven as good data hiding technique in past years. In my proposed work, a novel Steganographic Technique is proposed, which shows robustness against different types of attacks by utilizing the benefits of the properties of singular value decomposition, IWT and improved Voila Johns method for ROI. In purposed work I will try to gain obligatory and vibrant function of steganography in requisites of imperceptibility, complexity and advanced hiding capability. To evaluate performance of proposed work SNR, MSE, PSNR will be used.

1.1 Introduction

With the improvement of PC lot of facts receives transferred through net. Through internet with the help of pc records may be dispatched from one place to another location even in a second. Now a day the technology gets progressed. Whilst the cozy information is dispatched via any communiqué channel, it is able to be altered by using unauthorized individuals. The security measures desires to get better to tackle interception i.e. the unlawful alteration finished via illicit folks. Although, there are many technology exist for adequately switch of information like Cryptography, Watermarking, virtual signature, Fingerprinting and Steganography. One of the issues of information protection is the version of hidden change of data.[23]

Steganography is the talent of blanketed or hidden writing. Steganography is secret verbal exchange-to cover the even life of a message from outside world. Cover medium is the only wherein we hide the data by using stegonography algorithm we eliminates the pointless bits inside the cowl media and add the top secret records into that area. Better the pleasant of video or sound more redundant bits are available for hiding.

Different Steganography technique:

On the basis of interest of domain, steganography is classified as follows:

1. Spatial Domain Methods:

There are exceptional spatial steganography, all trade some of the bits within the photo pixel values in hiding information. One of the simplest techniques is Least significant bit (LSB)-based totally steganography that hides a secret information within the least good sized bits of pixel values without introducing many detectable distortions [24]. Adjustments within the cost of the LSB are unnoticeable for human eyes [25].

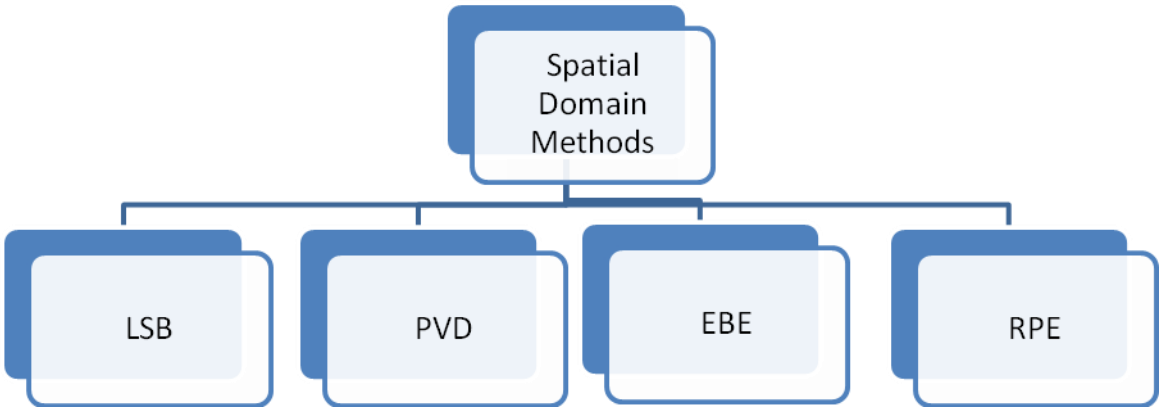

Fig.i: Spatial domain methods

2. *Transform Domain Technique:*

This is complicated way than spatial area technique of hiding facts in a photo. A ramification of algorithms and adjustments are used at the photograph to hide facts in it. Transform area concealing is likewise termed as a domain of concealing techniques for which a number of algorithms are counseled [26]. The technique of concealing information in the frequency area of a signal is secured than hiding ideas that function in the time domain. These techniques disguise facts in regions of the picture which are much less opened to firmness, cropping, and photograph processing. Some transform area strategies are can be lossless and lossy they're unbiased of video format [27] class of transform domain techniques:

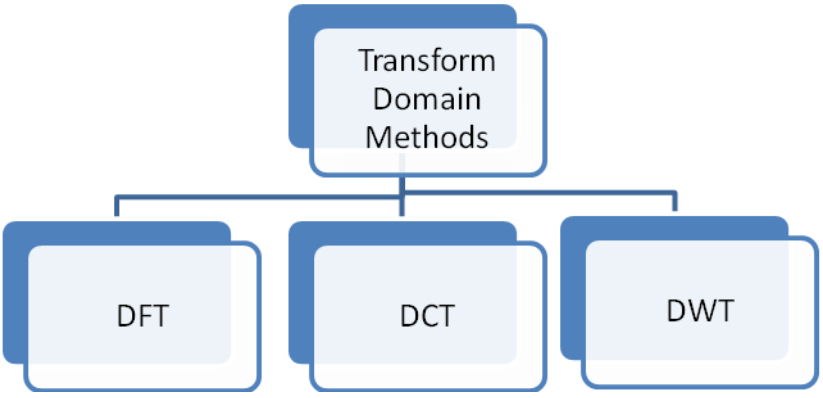

Fig.ii: Transform domain methods

On the basis of type of carrier chosen, Steganography is categorized as follows:

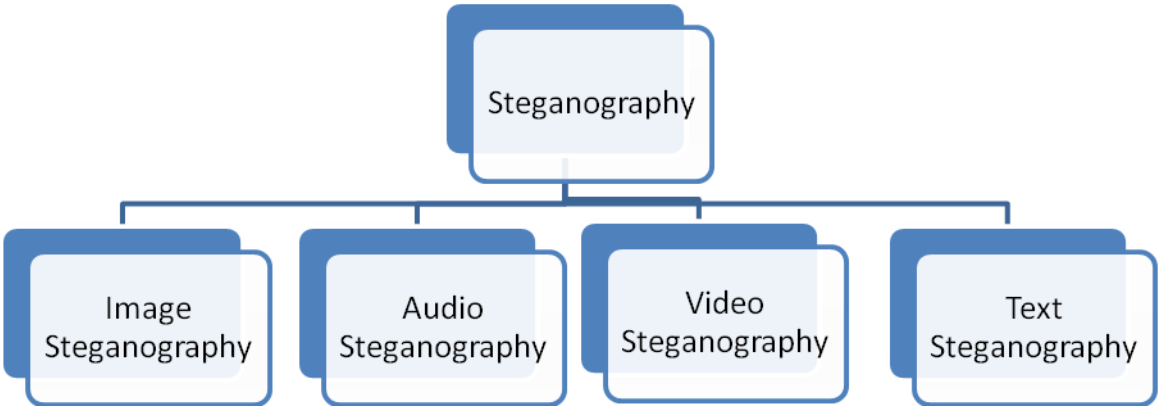

Fig.iii: Types of Steganography on basis of Cover File

1.2 Literature Review

Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. (1999) [1], hide data by using invisible ink. Invisible ink is used to mark certain letters in newspaper and also added sub-perceptible echo in audio at certain places then sent it to third party.

Maity, Santi P., and Malay Kumar Kundu. (2004) [2], information is embedded in grayscale image. A cryptic key is generated with the help of shift register. For transformation of image we apply Hadamard transformation on both cover and watermark image.Then Transform coefficients of cover and watermark image are arranged in rising order. At the end we apply Watson Visual and Entropy masking replica for modulation and information is embedded in cover image.

Çetin, Özdemir, and Ahmet TuranÖzcerit. (2009) [3], visible light spectrum is used to hide information in image. We find pixels in images that are having boundary values

(~380nm or ~750nm) of visible light spectrum on cover video frames, and then hide the secret information in those pixels. Those pixels with wavelength in the series of infrared or ultraviolet colors are invisible to human eyes. Human eyes cannot easily recognize minute modification at the visible light spectrum extremities.

Sherly, A. P., and P. P. Amritha. (2010) [4], information is concealed in macro blocks of I frame which leads to determined scene transform and in chunk of P and B frames which leads to supreme amount of motion vectors. By using this method we can expand the capacity of the concealed covert data and present an unnoticeable stego-image for human vision.

Mary, S., and Suma Christal. (2010) [5], information is hidden through audio steganography. It is based on real-time canceling of data. In this paper to hide information compressed video protected steganography (CVSS) algorithm is projected. In this technique, first compression is done by using Huffman algorithm and then information is concealed into cover audio message. At receiver end stego message is decoded. This paper employing statistical invisibility of contiguous frames.

Swathi, A., and S. A. K. Jilani. (2012): 1620-1623 [6], information is hidden inside video. Video is divided into images and then images are divided into frames and then by using polynomial equation we find the location where we can hide the information and then hide information with the help of LSB (least significant bit) technique.

Kelash, Hamdy M., et al. [7], author hide data in video clip by using color histogram, where every pixel in every video frame is separated into two parts, the bits which will be hidden in the right division are counted in the left division of pixel. This planned techniques has capability to hide huge amount of data, extracting the written text without errors, it also assurance integrity of framesto be extracted.

Hood, Ankita A., and N. J. Janwe. (2013) [8], PCA is mainly, used to optimize the algorithm. PCA remove correlation between the information. In combination with wavelet coefficient technique we use PCA for efficient hiding of information. Combination of both results in robust watermarking scheme.

Duluta, Andrei, et al. (2017) [9], a combination of encryption and image steganography is offered. Encryption is done by RSA algorithm and information is concealed in RGB components of color image using LSB. This paper consists of how covert message is concealed into a image carrier generating 3 unrelated but very similar images. Then these images are sending to the target using different communication channels and then used to recover the original message.

Apau, Richard. (2017) [10], first message is encrypted using RSA algorithm and then encrypted message is compressed with the help of Huffman encoding algorithm. By using LSB technique the compressed encrypted message is hidden into cover media. Lossless compression algorithm is applied so that size of message is reduced without loss of information.

Islam, Muhammad Nazrul,Fatima Jannat and Zinia Sultana. (2017) [11], two techniques are combined for security of secret information. First we have applied AES-128 for encryption of secret information and then this encrypted secret information is concealed in cover media by using LSB technique. For measuring performance of algorithm we used MSE and PSNR methods.

KumravatS. (2013) [12], photograph steganography is supplied that uses skin portion of an picture in DWT area for embedding of mystery information. Embedding of mystery records in handiest skin place decorates the safety and cropping is also help to hold degree of protection because without the cost of cropped region the message cannot be extracted. The proposed technique will provide better performance in phrases of PSNR.

Ma X, Li Z, Tu H, and Zhang B. (2010) [13], a robust video watermarking scheme with drift compression is proposed. The devised MB selection scheme can lower the impact on video great and reduce the opportunity of flow distortion. Within the meantime, a new waft compensation scheme is adopted to improve the imperceptibility of watermarking. Besides, the "strength compaction" property of DCT is applied to embed the watermark into motion vector residual with appropriate robustness towards intentional attack. The experimental effects imply that the video first-rate is sort of the same as that of the unique one, and the increase of bit price is less than zero.2%, which keeps the high video compression fee of h.264. This scheme is likewise strong towards malicious attack with distinctive QPS or motion estimation algorithms. Even with a high recompression fee of 80%, the correctness of watermark detection can nonetheless reach 70%.

Mansouri J, KhademiM. (2009) [14], A way of video steganography to secret message is projected in this content. Undisclosed facts were hidden in a compacted video bit circulation with temporal and spatial structures of the video signal. Concealing becomes executed by means of the thought of the human visible device uniqueness. By using this technique, every i-vop, blocks with great spatial modifications had been chosen and undisclosed information was concealed in few AC coefficients. For p-vop and b-vop, covert bits have been concealed in horizontal and vertical mechanism of movement vectors with great significance which characterized high temporal adjustments. Approach didn'tneed the unique bit movement

meant for records removal. The set of rules changed into carried out for unique bit prices and experimental outcomes indicated that this set of rules had high visible best and concealing ability. Furthermore, the bit rate remained almost regular without the usage of a bit time controller and this changed into some other benefit of the futuretechnique. Even though this set of rules changed into accomplished with superior easyreport in which every vop became the complete frame, this set of rules may be absolute to further shapes of mpeg-4 and to vop with a random form with insignificant variation.

Sadek M, Khalifa A, Mostafa MGM. (2014) [15], project a complete appraise of video steganographic strategies. An outline of steganography the use of exceptional cowl sorts becomes supplied and particularconsideration was rewarded to video steganography and to applications of video steganography. Diverse classification of the presentedsteganography techniques had been explained. A categorization is applied in keeping with the area of embedding, wherein techniques are labeled into three classes: spatial area strategies, transform area method, and different methods. Methods belonging to every area had been discussed and comparisons among the ones strategies had been offered highlighting their pros and cons. Besides, accepted picture and video fine metrics accessible inside the writing had been mentioned. In the end, steganalysis became surveyed from the factor of view that recovers the layout of accurate steganographic structures. A super and perfect video steganographic algorithm must offer massive hiding capability, excessive imperceptibility, robustness, and tamper resistance. However set of rules does now not survive in truth. Each and every one of the reviewed techniques had advantage and disadvantage that depend on the followed technique and the type of the software. So it's miles vital to make sure to facilitate one need to make use of the best set of rules for given application.

Eltahir ME, Kiah LM, Zaidan BB, Zaidan AA. (2009) [16], a present new move toward video steganography. The premise of this technique considers the virtual video record as disconnect frames and altering the output picture displayed on every video frame by secretedinformation that does not visually alternate picture. By this method, you will observe concealedmessage with greater area higher than different steganography media. In it 3-3-2 technique was practiced. Result have been a hit on extracted information of the video frames. End result was appropriate and the scale of statistics turned into enormous, round 33.3% from the dimensions of photograph. In different phrases, inside the liberty of five images, 500 pages of statistics might be saved without compression. In addition one second in sure video types incorporates about 27 frames which in turn creates masses of space for embedding statistics.

Sherly AP, AmrithaPP. (2010) [17], another video steganographic technique was planned in paper, working immediately in condensed area. To embed information tri-way pixel-value differencing (tpvd) set of rules were applied. These set of rules gives excessive potential and imperceptible stego-photograph for human vision of the concealedcovert statistics. Right here most scene change blocks have been framed to be used for embedding. The performance of the steganographic set of rules is calculated and investigational consequences suggests that technique can be functional on compressed videos with no great deprivation in visible exceptional.

Elgammal A, Muang C, Hu D. (2009) [18], the discussion was focused towards skin detection. Skin detection in blush pictures and videos is completely capable to perceive skin-colored pixels, may imply life of human faces and hands. Though, lots of items inside the actual world have skin-tone color, such as a few forms of leather-based, sandpaper, wooden, fur, and so on., which is probably mistakenly detected via a skin detector. Consequently, skin detection may be extremelyhelpful in locating human faces and fingers in restricted environments where in the background is assured not to include skin-tone coloration. Considering that pores and skin detection depends on locating pores and skin-colored pixels, its use is restricted to shade snap shots, i.e., it isn't always beneficial with grey-scale, infrared, or other kinds of photograph modalities that don't contain color facts. There enclose full-size studies on finding human faces in photos and videos the usage of different cues which include finding nearby facial structures or outcome holistic facial templates. Pores and skin detection can be used as an efficient preprocessing filter out to discover ability pores and skin areas in coloration snap shots former to relating more computationally luxurious face or hand detectors.

Channalli S, JadhavA. (2009) [19], The work provides a method which transmit massive portions of concealed message andpresent atease verbal exchange among two communicating parties. Steganography and cryptography techniques are used in this paper to make detection of hidden message more complex. Any manner of textual content records can be employed as covert data. The covertnoteusing the idea of steganography is dispatched through the network .In totaling, the planned system is simple and simple to put into effect. Also, the advanced gadget has many sensible, non-public and militaristic uses for both point-to-factor and point-to-multi-point interactions.

Method	Capacity	Robustness	Imperceptibility	Drawbacks
LSB	Work upto k=2 bits	k bits/pixel	Easy to detect	It is very simple method so easy to detect.
PVD	Work upto k=2 bits	<k bits/pixel	Easy to detect	It hide secret message in random pixels. So it provide better security than LSB method.
DWT	**Work upto k=4 bits**	**<k bits/pixel**	**Hardly Detectable**	**It works in time as well as frequency domain but co-efficient in this technique are in float numbers.**
DFT	Work upto k=4 bits	<k bits/pixel	Less chance of visibility of secret message	It works in time domain only.
IWT	**Work upto k=5 bits**	**>k bits/pixel**	**Undetectable secret message**	**It works in time as well as frequency domain and also it finds those areas that are less exposed to cropping, compression and image processing.**
DCT	Work upto k=4 bits	<k bits/pixel	Less chance of visibility of secret message	It works in frequency domain only

Table 1: Summary of Steganography techniques reviews

Magic Triangle:

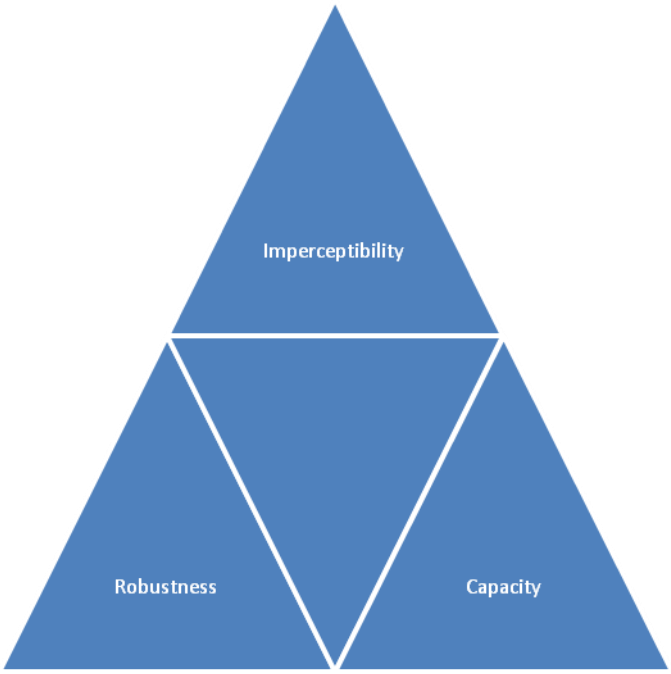

Fig.iv: Magic Triangle.

Imperceptibility

Steganography hide the secret statistics internal cover media. There are very less danger of visibility of modification completed through steganography method inside cover media. Imperceptibility means visibility of exchange inside the cover media. If our modified facts is having high Imperceptibility that means there are high hazard to detect hidden facts.

Robustness

It is the ability of the hidden message to remain unaltered and undamaged even if the stego file is subjected to various transformations.

Capacity

It is the ability to embed large size secret message.

The ultimate goal of steganography techniques is to achieve above **magic triangle**. A suitable method of video steganography that is accomplished by balancing between data hiding capacity, robustness while maintaining video quality and invisibility of exchange inside cover media. The above method of data hiding should be robust against attacks to make it useful for practical security strategies.

1.3 Problem Formulation Background

After a complete have look at the evaluation of cutting edge video steganography techniques and their overall concert opinions by literature review following Gaps are discovered in context of video steganography

1 An appropriate method of video steganography that is capable of balancing between data hiding capacity and robustness while maintaining video quality. It should be robust against attacks to make it useful for practical security strategies.

2 In order to achieve higher security, combination of steganography technique with some other data hiding and security techniques should be suggested. By applying a technique that put together steganography with other protection algorithm like cryptography and error correcting codes. As a consequence of this, the data would get pre processed (encrypt/encode) before embedding. This would ultimately increase security hence making attacks difficult for attacker during transmission.

3 Focusing on entire video to be a carrier while embedding results in degrades of quality. Thus it would be more beneficial if some specific portion of the video get targeted rather than entire video. Because of this the first challenge for attacker would be to find out the specific portion where message could have been embedded like face or body of human, cars and other objects similarly.

4 Using actual pixel domain as ROI for embedding, it would be better to use transformation coefficients. Due to this, the resulting steganogram would be extra robust aligned with signal processing and other compression methods.

1.4 Problem Formulation

ROI is frequently used to preserve crucial area of image. To guard critical components of image, the first-rate case is to preserve them in their distinctivestructure. Inside the real world, our plannedmethodalso be used to guard the crucial elements of photograph so that the ROI will no longer be damaged when covertmessage is fixed. First of all, we define ROI of image O, and along with that region plotis generated. The bitclear as “1”s in a vicinity plot represents the consequent pixel in ‘O’ as unfit for embedding. The others marked as bit “zero’s within the area plot imply that the consequent pixels inside the image O could be used to hold mystery facts. Although a place map is an auxiliary to facilitate with indicating which pixel is worth for embedding or not, the dimensions of vicinity plot is the indistinguishable.

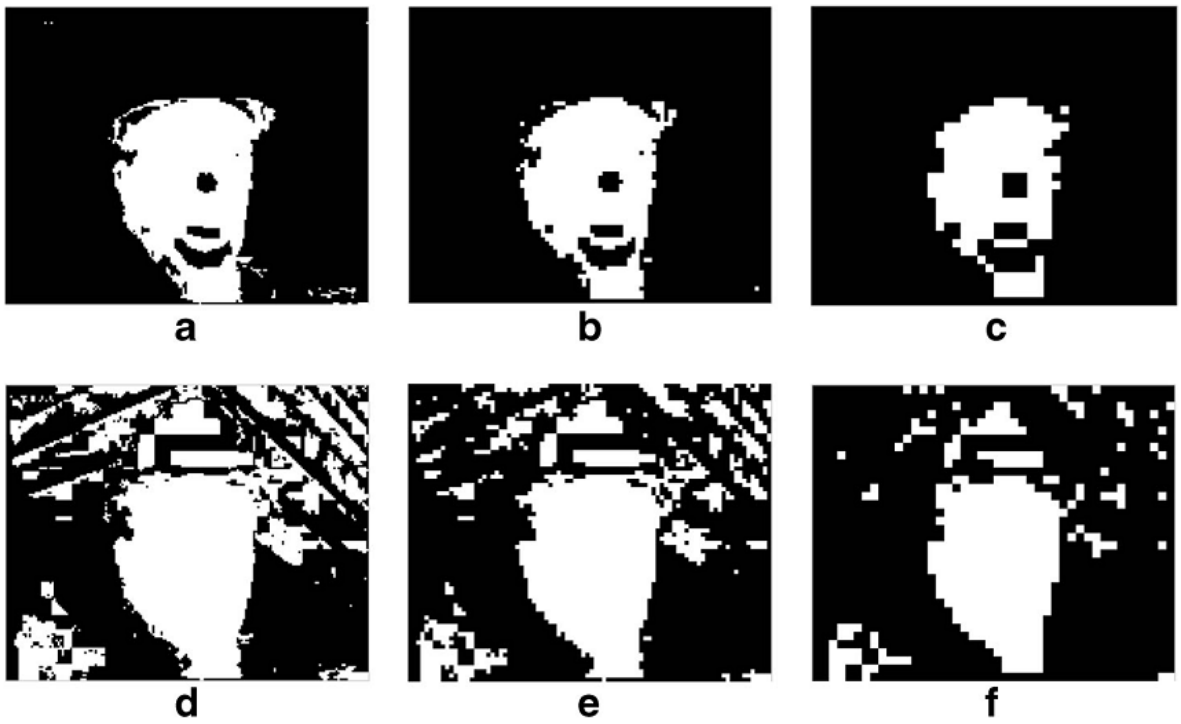

Fig.v: Unstable and Pixelated ROI Calculated using Skin detection [20]

Viola-Jones based object detection is definitely the state-of-the-art. It is one of best Object detection algorithms to run in real-time and is widely used for face detection. Also because it is still reliable and comes ready-to-use in a lot of image processing software packages like OpenCV. Both LBP and the Haar based approaches use an underlying Viola-Jones framework. The LBP approach uses a binary feature descriptor, represented as an unsigned integer. This results in: **Faster training time** and **object detection performance**, as binary feature representations (LBP) are faster to compute and process. Better tolerance to illumination variations compared to the Haar approach, as pixels are quantised to 0 or 1 depending on the "ratio" of pixel intensities and not the "actual" pixel intensities. However, the LBP approach approximates features (pixel quantization) and this result in the Haar approach producing more accurate results. The Viola-Jones with **Adaboost** approach offers real-time performance and scale/location invariance.

1. **Integral images** for rapid feature computation.
2. **Adaboost** to create strong classifiers (also known as feature selection).
3. Combine selected features into a **cascade structure** to get a **cascade classifier.** It is the cascade structure that makes the classifier extremely rapid.

1.4.1 DWT

“The wavelet transform can be viewed as a hierarchical sub-band system with sub-bandslogarithmically spaced in frequency. One dimensional Discrete Wavelet Transform(1D DWT) works by applying a low-pass filter and a high-pass filter to the input signalresulting in a low frequency band (L) and a high frequency band (H). When applied toimages, a two dimensional DWT extends the same approach by applying 1D DWT to therows and columns of the image successively. Four sub-bands are resulted: (HH)representing the diagonal features, (HL) and (LH) reflecting the vertical and horizontaldetails respectively and finally, (LL) representing the approximation version of the imageat half the resolution. The approximation imagecanbeusedfor further applicationof2DDWT generating more detail coefficients at different scales.Ontheother side, Inverse Discrete Wavelet Transform (IDWT) reconstructs the original imageusing the coefficients of all sub-bands” **[20].**

The discrete Fourier transform (DFT) tells you the frequency components of a signal, averaged over the entire duration of the signal. The discrete wavelet transform (DWT) gives information about the frequency (actually, basis) components as well as being able to indicate what time these components occur at.

1.5 IWT (Integer Wavelet Transforms) Domain Steganography

Using Wavelet remodel will in particular deal with the capability and robustness of data-embedding system characteristics. The Haar Wavelet rework is best of the entire wavelet remodel. DWT will produce coefficients in phrases of real factor numbers. Complexity of handling these coefficients with actual time gadget will be very high, which we can decrease with the aid of producing integer coefficients by IWT. Integer wavelet remodel can be obtained through lifting method. Lifting method is a way to transform DWT coefficients to Integer coefficients lacking dropping statistics. On this method the low frequency wavelet coefficients are produced by using averaging the 2 pixel values and high frequency coefficients are produced by system of taking half of the distinction of equal pixels. The four bands acquired are LL1, LH1, HL1, and HH1. The LL1 band is referred to as an approximation band, which includes low frequency wavelet coefficients, and consists of extensive a part of the spatial domain picture. Other bands are named as feature bands which contain high frequency coefficients and incorporate brink info of the spatial regionpicture.

1.5.1 Cons of DWT vs IWT

1. Greater complexity. Greater complication translates in this case into additional resources necessary to perform the computation - additional memory and/or processor cycles and/or time. If you don't need to locate events in time, or if the signal is stationary in the frequency domain, there is no advantage to DWT, and more effort to compute the values.
2. The theory is more difficult to understand. DFTs are much easier to understand, and are more intuitive. However, understanding enough to use a library function for DWTs is not much more difficult than learning to use a DFT routine, perhaps 2 or 3 times harder.
3. The flexibility of DWTs is a two-edged sword - it is sometimes very difficult to choose which basis to use. Do you need a differentiable basis? Then you won't want a Haar or low order Daubechies basis.
4. It is more difficult to interpret the results.

1.6 SVD

"Singular Value Decomposition transform is a linear algebra transform which is used for factorization of a real or complexmatrix with numerous applications in various fields of image processing [21]. As a digital image can be represented in amatrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimensions m x mis given by:

$$M = USV^T$$

Where, Uand V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non -negative singularvalues of matrix M.The columns of U and V are called left and right singular vectors of M, respectively. They basically specify the geometrydetails of the original image. Left singular matrix i.e., U represents the horizontal details and right singular matrix i.e. V represents the vertical details of the original image. The diagonal values of matrix S are arranged in decreasing order whichsignifies that importance of the entries is decreasing from first singular value for the last one, This feature is employed in SVD based compression techniques". Major benefits of SVD to utilize in digital watermarking methods [21]:

1 Littlemodification in singular values does not change the superiority of image and,

2 Singular values of image have very extraordinary firmness so; they do not alter after a range of attacks.

As Many SVD based steganographic techniques are proposed in the literature bydifferent authors. These SVD based steganographic techniques are robust to manydifferent types of attacks such as

1 Compression attack,

2 Cropping attack,

3 Impulse noise attack,

4 Gaussian attack and

5 Gamma correction attack

1.7 IWT-SVD vs DWT Steganography

The IWT-SVD watermarking technique may be carried out to make sure the copyright security and safety of data or images and to boom strength of picture. By using watermarking strategies and calculating PSNR value at distinct standards of scaling component (α), it could completed that the mixture IWT -SVD approach can provide moreimproved than easy DWT method as at each price of scaling component, cost of PSNR can be way extra in case of the mixed IWT-SVD method. Less cost of PSNR greater might be the degradation inside first-rate of authentic picture. This will be proven that following watermarking, the excellent of actualpicture degrades extra after easy DWT approach is used for hiding watermark in evaluation with IWT-SVD method hiding[22].

On evaluating values of PSNR at diversestandards of scaling component C, could be proven that the mixed method IWTSVD is an awful lot superiorthan DWT method. As at all price of scaling thing, value of top PSNR is greater in hybrid method. Less the fee of PSNR more triggered degradation within the best of authentic photo. This indicates that following watermarking, first-class of authentic picture degrades greater while DWT approach is used for hiding the watermark in evaluation with IWT-SVD approach hiding [21].

1.8 Proposed Work and Methodology

The necessities of steganography methods are majorly alarmed with perceptual invisibility, Statistical invisibility in addition tomassive payloads. Because of this reason our most important purpose of this work is towards gain of maximum decisive, obligatory and vital

function of steganography in requisites of imperceptibility, complexity and advanced hiding capability. Our studies investigate a few progressive methods to improve video steganography techniques. Primary goal of this work is to increase and authenticate a new technique to do better than the prevailing video steganography strategies from the literature review. Suggestions and guidelines are provided to design efficient video steganography, that is the principle motivation of this paintings using IWT-SVD which first-rate appropriate for remodel domain Steganography with ROI extraction the use of Improved Voila Johns approach the usage of Adaboost.

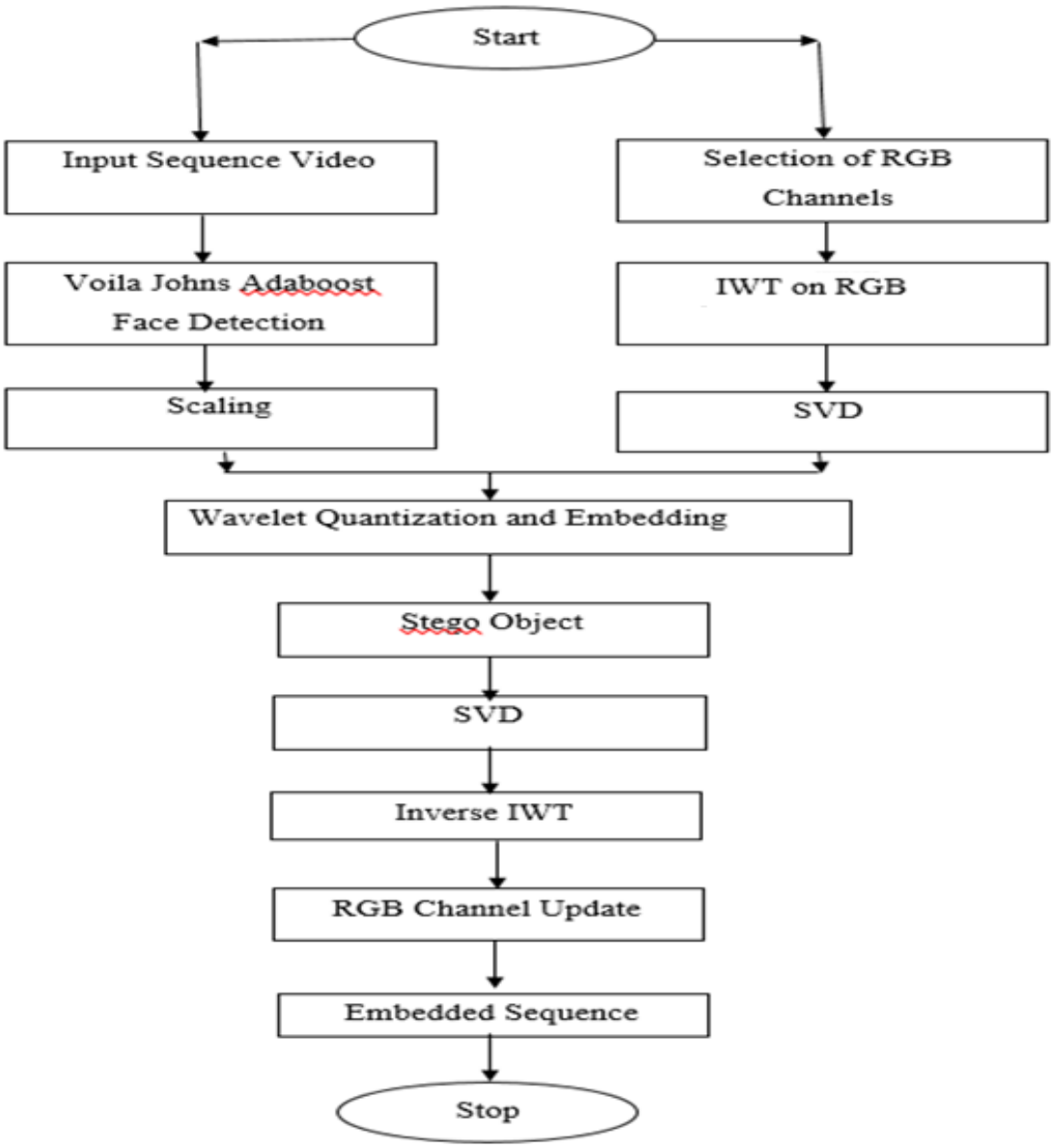

Fig. vi: Working of Proposed ROI based Scheme

In proposed work, the key contributions are as follows:

- A particularly relaxed video steganography set of rules primarily based on stepped forward ROI Extraction is proposed. if you want to beautify the safety and robustness of this set of rules towards attacks, the secret message is concealed into unique areas of every video frame, arbitrarily. The set of rules achieves improved imperceptibility of stego video as well as superior concealing capacity of covertinformation.
- In order to calculate stable ROI, Improved **Voila Johns** Method using Adaboost Cascades is used which is advancement to the previous works [21].
- An improved payload video steganography method inside the discrete wavelet area based totally on SVD is planned. This technique now not best enhanced the capability of the encoded covert information, but additionally elevated the strengthnext to attacks, supplying an affordable exchange with imperceptibility.
- This algorithm utilizes more than one motion items (Human Faces) inside the video frames as areas of hobby to conceal the covert statistics, which operates within the spatial domain. The above techniqueenhances imperceptibility and concealing ability when compared to associated video steganography techniques.
- A strong and comfortable video steganography set of rules into IWT-SVD domains are proposed in turn affords a better confidentiality to the name of the game communication prior to concealing segment. In organize to decorate safety and strength of the proposed method, each wavelet and cosine frequency coefficients of shifting items all the way through the video frames are applied as host information to hide the name of the game communication.
- ROI Calculations are done using Improved **Voila Johns** method.

1.9 Research Objectives

1. Study and Analyze Various Steganographic Approaches find out their weaknesses and strengths.
2. To Propose a Steganographic technique, which shows robustness against different types of attacks which takes the advantages of the properties of singular value decomposition, Robustness and Capacity of IWT with Stable ROI calculation using improved Voila Johns method for Face detection.
3. To Evaluate the Performance of Proposed Work using MSE, PSNR, SSIM , Capacity etc.

1.10 Tools and Techniques

For the above said research work, we will be requiring to access the various e-journals like IEEE, Science Direct and ACM. For data collection and analysis of the data, I will be requiring various software's and Internet facility. The hardware and software requirements for my thesis work are

Hardware Requirements:

- Processor: i3 or Higher
- RAM: 4 GB or Higher
- Hard Disk: 250 GB or Higher

Software Requirements:

- Platform: Windows 7 Professional
- MATLAB 2016b and above
- Microsoft office(Excel and Word)

1.11 References

[1]. Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information hiding-a survey." Proceedings of the IEEE 87.7 (1999): 1062-1078.

[2]. Maity, Santi P., and Malay Kumar Kundu. "An image watermarking scheme using HVS characteristics and spread transform." Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on. Vol. 4. IEEE, 2004.

[3]. Çetin, Özdemir, and Ahmet TuranÖzcerit. "A Blind Video-Steganography Technique Based on Visible Light Wavelength for Raw Video Streams." (2009): 385-389.

[4]. Sherly, A. P., and P. P. Amritha. "A compressed video steganography using TPVD." International Journal of Database Management Systems (IJDMS) Vol 2.3 (2010).

[5] Mary, S., and Suma Christal. "IMPROVED PROTECTION IN VIDEO STEGANOGRAPHY USED COMPRESSED VIDEO BITSTREAMS." International Journal on Computer Science and Engineering 2.3 (2010).

[6]. Swathi, A., and S. A. K. Jilani. "Video steganography by LSB substitution using different polynomial equations." International Journal of Computational Engineering Research (ijceronline. com) Vol 2 (2012): 1620-1623.

[7]. Kelash, Hamdy M., et al. "Hiding data in video sequences using steganography algorithms." ICT Convergence (ICTC), 2013 International Conference on. IEEE, 2013.

[8]. Hood, Ankita A., and N. J. Janwe. "Hiding Data in Video Using Discrete Wavelet Transform And Principal Component Analysis." International Journal of Engineering 2 (2013): 1165-1169.

[9]. Duluta, Andrei, et al. "Secure Communication Method Based on Encryption and Steganography" Control Systems and Computer Science (CSCS), 21st International Conference on IEEE, 2017

[10]. Apau, Richard,"Enhancing Data Security using Video Steganography, RSA and Huffman CodeAlgorithms with LSB Insertion", Diss. 2017.

[11]. Islam, Muhammad Nazrul,Fatima Jannat and Zinia Sultana. " A New Approach to Hide Data in Color ImageUsing LSB Steganography Technique", 3rd International Conference on Electrical Information and Communication Technology (EICT), 7-9 December 2017, Khulna, Bangladesh.

[12]. KumravatS ,"An efficient steganographic scheme using skin tone detection and discrete wavelet transformation",Int Journal Computer Science Engineering Technology (IJCSET) (2013)

[13]. Ma X, Li Z, Tu H, and Zhang B ,"A data hiding algorithm for H.264/AVC video streams without intraframedistortion drift", IEEE transactions on circuits and systems for video technology (2010).

[14]. Mansouri J, KhademiM ,"An adaptive scheme for compressed video steganography using temporaland spatial features of the video signal",Int J Imaging SystTechnol 19(4):306–315(2009)

[15]. Sadek M, Khalifa A, Mostafa MGM ,"Video steganography a comprehensive review",Multimed ToolsAppl. (2014) doi:10.1007/s11042-014-1952-z

[16]. Eltahir ME, Kiah LM, Zaidan BB, Zaidan AA," High rate video streaming steganography", International Conference on Future Computer and Communication (ICFCC 2009) 672–675(2009)

[17]. Sherly AP, AmrithaPP ,"A compressed video steganography using TPVD",Int J Database Management System(2010). doi: 10.5121/ijdms.2010.230767

[18].Elgammal A, Muang C, Hu D," Skin detection - a short tutorial", In Encyclopedia of Biometrics. 1218–1224. Springer US(2009).

[19]. Channalli S, JadhavA,"Steganography an art of hiding data ",Int J ComputSci Eng 1(3):137–141 (2009).

[20]. Mennatallah M. Sadek, Amal S. Khalifa, Mostafa G. M. Mostafa,"Robust video steganography algorithm using adaptive skin-tone detection", Multimedia Tools and Applications, 2017, Volume 76, Number 2, Page 3065.

[21]. http://en.wikipedia.org/wiki/Singular_value_decomposition.

[22]. Neha Narula , Deepak Sethi and ParthaPratim Bhattacharya," Comparative Analysis of DWT and DWT-SVD Watermarking Techniques in RGB Images", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8, No. 4 (2015), pp. 339-348.

[23]. Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information hiding-a survey." Proceedings of the IEEE 87.7 (1999): 1062-1078.

[24]. Liu, Chiang-Lung, and Shiang-Rong Liao. "High-performance JPEG steganography using complementary embedding strategy." Pattern Recognition 41.9 (2008): 2945-2955.

[25]. Biradar, DrRajkumar L., and AmbikaUmashetty. "A Survey Paper on Steganography Techniques." International Journal of Innovative Research in Computer and Communication Engineering (A High Impact Factor, Monthly, Peer Reviewed Journal) Vol 4 (2016).

[26]. Maharshi, Amit, Ravindra Prakash Gupta, and Vijay Mohan Shrimal. "Simulation based watermarking for confidential data security for video signal." *International Journal* 2.1 (2012).

[27]. Chandel, Bharti, and Shaily Jain. "Video Steganography: A Survey." *IOSR Journal of Computer Engineering* 18 (2016).

MANAV RACHNA
Vidyaparikshan

Swami Vivekananda Library and Resource Centre
Manav Rachna University

SIMILARITY VERIFICATION CERTIFICATE

Title: An Optimized Steganography Techniques using Hybrid Approach

Researcher : URMILA PILANIA Registration Number: MRU00745

Supervisor: Dr. PRINIMA GUPTA Department: CST

This is to certify that the above mentioned Short Synopsis /~~Thesis~~ was scanned for similarity index through Turnitin Software on 16 Aug, 18 with submission ID 990372900 and the similarity index was found to be 4%. The complete report running into 20 Pages, 4799 Word count with File Size 4092 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

Swami Vivekananda Library and Resource Centre, Faridabad * Manav Rachna University * 16/8/2018

Date: 16 August, 2018

The complete report of the above Short Synopsis/~~Thesis~~ has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/~~Thesis~~ may be considered for further processing.

Urmila 16/8/2018
Research Scholar

16/8/2018
Research Supervisor

Urmila_Synopsis_16Aug_-_Copy.doc

by

Submission date: 16-Aug-2018 08:39PM (UTC+0530)
Submission ID: 990442981
File name: Urmila_Synopsis_16Aug_-_Copy.doc (354K)
Word count: 4897
Character count: 26941

Proposed Title: A Novel Steganography Technique using ROI, IWT and SVD

Abstract: In today's world of internet most of the data travel through internet. It is desirable to secure the information at sender's end till it reaches receiver's end and during transmission. Today everybody is using internet that may be a child or may be an old age person, every professional is using internet to create digital data and that data is shared over the network, as so many people's are using internet so information security has become a prime task. That is why we need some security techniques for safety of information during information travel over the internet. There are some techniques for protection of data like Cryptography, Watermarking, Digital Signature and Steganography. Steganography has been proven as good data hiding technique in past years. In my proposed work, a novel Steganographic Technique is proposed, which shows robustness against different types of attacks by utilizing the benefits of the properties of singular value decomposition, IWT and improved Voila Johns method for ROI. In purposed work I will try to gain obligatory and vibrant function of steganography in requisites of imperceptibility, complexity and advanced hiding capability. To evaluate performance of proposed work SNR, MSE, PSNR will be used.

1.1 Introduction

With the improvement of PC lot of facts receives transferred through net. Through internet with the help of pc records may be dispatched from one place to another location even in a second. Now a day the technology gets progressed. Whilst the cozy information is dispatched via any communiqué channel, it is able to be altered by using unauthorized individuals. The security measures desires to get better to tackle interception i.e. the unlawful alteration finished via illicit folks. Although, there are many technology exist for adequately switch of information like Cryptography, Watermarking, virtual signature, Fingerprinting and Steganography. One of the issues of information protection is the version of hidden change of data.[23]

Steganography is the talent of blanketed or hidden writing. Steganography is secret verbal exchange-to cover the even life of a message from outside world. Cover medium is the only wherein we hide the data by using stegonography algorithm we eliminates the pointless bits inside the cowl media and add the top secret records into that area. Better the pleasant of video or sound more redundant bits are available for hiding.

Short

Urmila_Synopsis

ORIGINALITY REPORT

Excluding matches less than 14 words

4%	1%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to VIT University Student Paper	1%
2	Driss Matrouf, Jean-François Bonastre. "Chapter 201 Session Effects on Speaker Modeling", Springer Nature, 2015 Publication	1%
3	"Contemporary Computing", Springer Nature America, Inc, 2012 Publication	1%
4	Pathak, Yatindra, and Satish Dehariya. "A more secure transmission of medical images by two label DWT and SVD based watermarking technique", 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), 2014. Publication	1%
5	Sadek, Mennatallah M., Amal S. Khalifa, and Mostafa G. M. Mostafa. "Video steganography: a comprehensive review", Multimedia Tools and Applications, 2015. Publication	<1%

Exclude quotes On

Exclude bibliography On

Exclude matches Off